UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,503	11/02/2000	David J. Wetherall	0016.0005US1	8089

29127 7590 10/18/2010

HOUSTON ELISEEVA
420 BEDFORD ST
SUITE 155
LEXINGTON, MA 02420

EXAMINER	
BIAGINI, CHRISTOPHER D	
ART UNIT	PAPER NUMBER
2445	

MAIL DATE	DELIVERY MODE
10/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/706,503	WETHERALL ET AL.	
	Examiner	Art Unit	
	Christopher D. Biagini	2445	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/17/2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,14,16,42-45,47,48,51-54 and 58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3, 14, 16, 42-45, 47, 48, 51-54, and 58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to the amendment filed August 17, 2010. Claims 1, 3, 14, 16, 47, 48, and 58 were amended. Claims 5-13, 18-27, 29, 31-39, 56, 57, and 59 were cancelled. Claims 1, 3, 14, 16, 42-45, 47, 48, 51-54, and 58 are pending.

Response to Arguments

Applicant's arguments with respect to the rejections of claims 1, 3, 5, 10-16, 18, 27, 29, 31, 36-39, 42, 43, 47, 41, 42, 56, and 58 under 35 USC 103(a) over Malan, Poletto, and Katoh have been fully considered and are technically moot in view of the new ground(s) of rejection.

However, with respect to the applicability of Li to the claimed invention, Applicant argues that "only the Li shows a two router system" and, since "the pending claims are directed to more than simply the concept of using to routers," the claimed "functionality is neither shown nor suggested by any of the applied references. The Examiner respectfully disagrees. As explained in the previous rejection of claim 6, the system of Malan monitors the entire "routing infrastructure" (see first paragraph under "StormProfiler" on p. 11, and figures on pp. 17-19, indicating collecting traffic statistics from multiple routers). However, Malan does not *explicitly* show that another of the routing devices is for routing network traffic out of and into the first network domain. Li, on the other hand, shows a network domain comprising a second routing device for routing network traffic out of and into the network domain (see col. 7, lines 30-45). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify

the system of Malan in view of Poletto and Katoh with the second routing device taught by Li in order to reduce the burden on the first routing device.

Accordingly, Applicant's arguments cannot be held as persuasive.

Applicant's arguments with respect to the rejection of claim 48 under 35 USC 103(a) over Malan in view of Ko have been fully considered but are not persuasive.

Applicant argues that the "The functionality from the Ko patent bears no relationship to the present claimed invention" and that "Ko is merely concerned with obtaining information concerning password tries reported by host computers." The Examiner respectfully disagrees. Ko, like the present invention, is concerned with detecting large-scale attacks on a network infrastructure (see col. 5, lines 20-22: "Analysis module 204 gathers and correlates information reported by sensors and lower-level analyzers to infer occurrences of large-scale attacks.") Also like the current invention, Ko contemplates lowering a threshold for concluding that a network attack is occurring at a network domain (parameters sent to lower-level sensors "can be changed to more conservative values during an attack": see col. 5, lines 16-17). In other words, Ko detects when an attack is occurring at one location, concludes that it may be part of a larger-scale attack, and tunes the system to be more sensitive for attacks occurring at other locations. In the example given, the system concludes that fewer password tries are necessary to trigger a security response during an attack.

Applicant's arguments with respect to claim 58 correspond to the arguments addressed above in connection with claim 48. The Examiner disagrees for at least the reasons given above

Accordingly, Applicant's arguments cannot be held as persuasive.

Claim Objections

Claim 48 objected to because of the following informalities: the claim introduces the limitation "a second network domain" twice, and later refers to "the second network domain": see lines 3 and 7-8. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 14, 16, 42, 43, 47, 51, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Katoh (US Patent No. 5,949,757), Li (US Patent No. 5,473,599), and Ko (US Patent No. 6,7879,202).

Note that Malan claims priority to and incorporates by reference three provisional applications: Nos. 60/231,479, 60/231,480, and 60/231,481, all filed on September 8, 2000. Except where noted below, all page and line numbers cited in connection with Malan refer to those in application No. 60/231,680. Since the numbering of the pages is inconsistent throughout the application, the numbers will refer to the pages as they were scanned into the PTO records (i.e., with page 1 being the cover sheet).

Similarly, Poletto claims priority to and incorporates by reference provisional application No. 60/230,759, filed September 7, 2000. Except where noted below, all page and line numbers cited in connection with Poletto refer to those in application No. 60/230,759. Since the numbering of the pages is consistent throughout the application, the numbers will refer to the pages as they are labeled (i.e., with page 1 corresponding to the third scanned sheet in the application).

Regarding claim 1, Malan shows:

- a first network domain (for example, an enterprise network: see first paragraph under "StormDetector" on p. 12);
- a first routing device (comprising an attacker's router) at a boundary between the first network domain and public internetworking fabric (comprising an ISP network: see Fig. 4 and the paragraph spanning pp. 14-15) to route network traffic between the first network domain and the public internetworking fabric (implicitly disclosed as the typical functionality of a first-hop router: see last paragraph on p. 12);
- a second routing device for routing network traffic (another of the routers depicted in Fig. 4 and figures on pp. 17-19);
- a monitor/regulator (comprising the StormDetector analysis engine), either integrally disposed in said first routing device or coupled to the first routing device (see second paragraph under "StormDetector" on p. 12 and Figs. 2 and 4) to monitor the network traffic routed by said first routing device and said second routing device (see first paragraph under "StormProfiler" on p. 11, and figures on pp. 17-19, indicating

collecting traffic statistics from multiple routers) by analyzing flow records (comprising "flow statistics": see second and third paragraphs under "StormDetector" on p. 12 and note that StormDetector can be used in "source and transit networks" and "an attacker's originating network"), each describing a traffic conversation as indicated by a combination of source and destination addresses (comprising "flow statistics" as described above, further explained as being indicated by a combination of source and destination addresses in the paragraph spanning pp. 3-4), received from the first routing device and the second routing device (note that the analysis engine receives flow statistics from all the routers in the attack path, including the attacker's router: see "StormProfiler" on p. 11), the monitor/regulator determining if the first network domain is sourcing undesirable network traffic (comprising determining that the attack originates in the enterprise network: see paragraph spanning pp. 14-15), comprising a denial of service attack in which the undesirable network traffic is launched against a target network device (for example, a target web hosting server: see "StormDetector" on p. 12 and "StormBreaker" on p. 14) in order to undermine the operation of that target network device by overwhelming the target network device with network traffic (typical of denial of service attacks, and further explained at the first paragraph on p. 3), out of the first network domain (note that the attacker must send the traffic out of the enterprise network in order for it to reach the web host) based on the network traffic being routed by said first routing device and said second routing device (see first paragraph under "StormProfiler" on p. 11, and figures on pp. 17-19, indicating collecting traffic statistics from multiple routers);

- wherein said monitor/regulator makes said determination based on aggregated network traffic ("flow statistics": see second and third paragraphs under "StormDetector" on p. 12) routed by the first routing device and the second routing device (see "StormDetector" on p. 12, and note that StormDetector "instantly identify[ies] malicious traffic" and can be "employed at an attacker's originating network"; see also first paragraph under "StormProfiler" on p. 11, and figures on pp. 17-19, indicating collecting traffic statistics from multiple routers), and
- wherein said monitor/regulator instructs the first routing device to mitigate the undesirable network traffic (by "blocking" it) that is being sourced from the first network domain in response to making said determination that the first network domain is sourcing the undesirable network traffic (see discussion of "StormBreaker" at p. 14).

Malan does not *explicitly* show wherein said monitor/regulator makes said determination based at least in part on differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

Poletto shows identifying malicious traffic at a routing device (comprising a gateway) based on differential characteristics (comprising a ratio of request packets to acknowledgement packets) between request packets routed out of said network domain (comprising client request packets which are routed out of an attacker's domain), and response packets routed into the network domain (comprising server acknowledgement packets which are routed into the attacker's domain: see pages 15-16). Because both Malan and Poletto teach methods for

identifying malicious traffic at a routing device, it would have been obvious to one of ordinary skill in the art to substitute one method for the other in order to achieve the predictable result of determining that the network domain is sourcing undesirable traffic.

Malan in view of Poletto does not explicitly show wherein the instruction to mitigate the undesirable network traffic is to lower the priority of the undesirably network traffic.

Katoh teaches lowering the priority of undesirable traffic as an alternative to blocking it outright (see col. 4, lines 10-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto to lower the priority of undesirable traffic as taught by Katoh in order to ease congestion caused by the attack without running the risk of blocking innocent traffic entirely.

Malan in view of Poletto and Katoh does not *explicitly* show that the second routing device is for routing network traffic out of and into the first network domain.

Li shows a network domain comprising a second routing device for routing network traffic out of and into the network domain (see col. 7, lines 30-45). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto and Katoh with the second routing device taught by Li in order to reduce the burden on the first routing device.

Malan in view of Poletto, Katoh, and Li does not explicitly show that the monitor/regulator instructs both the first and second routing devices.

Ko shows sending instructions to multiple network devices in a single network domain (local analyzers and sensors, of which there can be more than one in a single network domain: see col. 5, lines 38-54 and, in Fig. 2, depiction of sensors 140 and 141 in local network 108) to

stop undesirable traffic (see col. 2, lines 46-52) when mitigating a large-scale network attack (see col. 5, lines 20-34 and col. 7, lines 6-21). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto, Katoh, and Li to send the instructions to both the first and second routing devices in order to ensure that all devices responsible for the network traffic are able to quickly react to an on-going large-scale attack while maintaining consistency with a global policy (see Ko, col. 5, lines 43-46).

Regarding claim 3, the combination further shows wherein said monitor/regulator infers said differential characteristics based on aggregated statistics of said network traffic routed out of said first network domain by said first routing device and said second routing device, and aggregated statistics of said network traffic routed into the first network domain by said first routing device and said second routing device (comprising maintaining an analysis of the ratio "over time": see Poletto, middle of page 13, "traffic is monitored at multiple levels of granularity, from aggregate to individual flows" and "Multi-level analysis can be applied to all types of monitoring (i.e. TCP packet ratios...)"; see also discussion of maintaining the ratios at pp. 15-16: the monitoring process examines "a ratio of incoming to outgoing number of TCP packets for a particular set of machines" and "can store 86 this ratio, time stamp it, etc. and conduct an ongoing analysis 88 to determine over time for example how much and how often it exceeds that ratio"). Note that as combined above, the monitoring process of Poletto is executing on the routers of Malan, including the first and second routers (see first paragraph under "StormProfiler" on p. 11 of Malan, and figures on pp. 17-19, indicating collecting traffic statistics from multiple routers). Thus, request packets from the attacker would be routed out of

the attacker's network domain (such as the enterprise network), and response packets would be routed into the attacker's network domain.

Regarding claim 42, the combination further shows wherein said monitor/regulator generates statistics concerning destination addresses and determines whether the first network domain is sourcing undesirable network traffic based on said statistics (see discussion of "flow-based statistics," including "destination address," in paragraph spanning pp. 3-4 of Malan).

Regarding claim 43, the combination further shows wherein said monitor/regulator generates statistics concerning lengths of packets and determines whether the first network domain is sourcing undesirable network traffic based on said statistics (see discussion of "single packet statistics," including "length," in paragraph spanning pp. 3-4 of Malan).

Regarding claim 47, the combination further shows wherein said monitor/regulator instructs said first routing device and said second routing device to slow the undesirable network traffic (comprising slowing the attack traffic to zero with instructions to the routers that block traffic as explained above: see paragraph spanning pp. 14-15 of Malan and col. 7, lines 17-22 of Ko).

Regarding claim 14, Malan shows a network traffic regulation method comprising:

- monitoring network traffic routed by a first routing device (comprising an attacker's router) of a first network domain (for example, an enterprise network: see first paragraph under "StormDetector" on p. 12);
- monitoring network traffic routed by a second routing device (another of the routers depicted in Fig. 4 and figures on pp. 17-19);
- determining if the first network domain is sourcing undesirable network traffic (comprising determining that the attack originates in the enterprise network: see paragraph spanning pp. 14-15), comprising a denial of service attack in which the undesirable network traffic is launched against to a target network device (for example, a target web hosting server: see "StormDetector" on p. 12 and "StormBreaker" on p. 14) in order to undermine the operation of that target network device by overwhelming the target network device with network traffic (typical of denial of service attacks, and further explained at the first paragraph on p. 3), out of the first network domain (note that the attacker must send the traffic out of the enterprise network in order for it to reach the web host), wherein the first network domain is determined to be sourcing undesirable network traffic by analysis of flow records (comprising "flow statistics": see second and third paragraphs under "StormDetector" on p. 12 and note that StormDetector can be used in "source and transit networks" and "an attacker's originating network") describing traffic conversation, as indicated by a combination of source and destination addresses (comprising "flow statistics" as described above, further explained as being indicated by a combination of source and destination addresses in the paragraph spanning pp. 3-

4), received from the first routing device and the second routing device (note that the analysis engine receives flow statistics from all the routers in the attack path, including the attacker's router: see "StormProfiler" on p. 11), the first network device is positioned at a boundary between the first network domain and public internetworking fabric to route network traffic between the first network domain and the public internetworking fabric (implicitly disclosed as the typical functionality of a first-hop router: see last paragraph on p. 12);

- wherein said determining comprises determining based on aggregated network traffic ("flow statistics": see second and third paragraphs under "StormDetector" on p. 12) routed by the first routing device and the second routing device (see "StormDetector" on p. 12, and note that StormDetector "instantly identify[ies] malicious traffic" and can be "employed at an attacker's originating network"; see also first paragraph under "StormProfiler" on p. 11, and figures on pp. 17-19, indicating collecting traffic statistics from multiple routers); and
- mitigating the undesirable network traffic (by "blocking" it) that is being sourced from the first network domain and routed by said first networking device in response to making said determination that the first network domain is sourcing the undesirable network traffic (see discussion of "StormBreaker" at p. 14).

Malan does not *explicitly* show making said determination based at least in part on differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

Poletto shows identifying malicious traffic at a routing device (comprising a gateway) based on differential characteristics (comprising a ratio of request packets to acknowledgement packets) between request packets routed out of said network domain (comprising client request packets which are routed out of an attacker's domain), and response packets routed into the network domain (comprising server acknowledgement packets which are routed into the attacker's domain: see pages 15-16). Because both Malan and Poletto teach methods for identifying malicious traffic at a routing device, it would have been obvious to one of ordinary skill in the art to substitute one method for the other in order to achieve the predictable result of determining that the network domain is sourcing undesirable traffic.

Malan in view of Poletto does not explicitly show mitigating the undesirable network traffic by lowering the priority of the undesirably network traffic.

Katoh teaches lowering the priority of undesirable traffic as an alternative to blocking it outright (see col. 4, lines 10-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto to lower the priority of undesirable traffic as taught by Katoh in order to ease congestion caused by the attack without running the risk of blocking innocent traffic entirely.

Malan in view of Poletto and Katoh does not *explicitly* show that the second routing device is "of said first network domain" and is positioned at the boundary of the first network domain

Li shows a network domain comprising a second routing device which is at the boundary of the network domain and is for routing network traffic between the network domain and another network (see col. 7, lines 30-45). It would have been obvious to one of ordinary skill in

the art at the time of the invention to modify the system of Malan in view of Poletto and Katoh with the second routing device taught by Li in order to reduce the burden on the first routing device.

Malan in view of Poletto, Katoh, and Li does not explicitly show lowering the priority of traffic that is being routed by both the first and second networking devices.

Ko shows sending instructions to multiple network devices in a single network domain (local analyzers and sensors, of which there can be more than one in a single network domain: see col. 5, lines 38-54 and, in Fig. 2, depiction of sensors 140 and 141 in local network 108) to stop undesirable traffic (see col. 2, lines 46-52) when mitigating a large-scale network attack (see col. 5, lines 20-34 and col. 7, lines 6-21). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto, Katoh, and Li to send the instructions to both the first and second routing devices in order to ensure that all devices responsible for the network traffic are able to quickly react to an on-going large-scale attack while maintaining consistency with a global policy (see Li, col. 5, lines 43-46).

Regarding claim 16, the combination further shows wherein said monitor/regulator infers said differential characteristics based on aggregated statistics of said network traffic routed out of said first network domain by said first routing device and said second routing device, and aggregated statistics of said network traffic routed into the first network domain by said first routing device and said second routing device (comprising maintaining an analysis of the ratio "over time": see Poletto, middle of page 13, "traffic is monitored at multiple levels of granularity, from aggregate to individual flows" and "Multi-level analysis can be applied to all

types of monitoring (i.e. TCP packet ratios...)"; see also discussion of maintaining the ratios at pp. 15-16: the monitoring process examines "a ratio of incoming to outgoing number of TCP packets for a particular set of machines" and "can store 86 this ratio, time stamp it, etc. and conduct an ongoing analysis 88 to determine over time for example how much and how often it exceeds that ratio"). Note that as combined above, the monitoring process of Poletto is executing on the routers of Malan, including the first and second routers (see first paragraph under "StormProfiler" on p. 11 of Malan, and figures on pp. 17-19, indicating collecting traffic statistics from multiple routers). Thus, request packets from the attacker would be routed out of the attacker's network domain (such as the enterprise network), and response packets would be routed into the attacker's network domain.

Regarding claim 51, the combination further shows wherein said monitor/regulator generates statistics concerning destination addresses and determines whether the first network domain is sourcing undesirable network traffic based on said statistics (see discussion of "flow-based statistics," including "destination address," in paragraph spanning pp. 3-4 of Malan).

Regarding claim 52, the combination further shows wherein said monitor/regulator generates statistics concerning lengths of packets and determines whether the first network domain is sourcing undesirable network traffic based on said statistics (see discussion of "single packet statistics," including "length," in paragraph spanning pp. 3-4 of Malan).

Claims 44 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Katoh (US Patent No. 5,949,757), Li (US Patent No. 5,473,599), Ko (US Patent No. 6,7879,202), and Carr (US Patent No. 5,293,379).

Regarding claim 44, the combination further shows wherein said monitor/regulator generates statistics concerning distributions of various fields in TCP/IP packet headers (see discussion of "single-packet statistics" in paragraph spanning pp. 3-4 of Malan) and determines whether the first network domain is sourcing undesirable network traffic based on said statistics, but does not show that the statistics are generated using time to live values.

Carr shows that TCP/IP packet headers include time to live values (see Fig. 4 and col. 5, lines 27-36). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto, Katoh, Li, and Ko to use the TTL field taught by Carr along with the statistics generation taught by Malan in order to provide an additional basis for determining that traffic is malicious.

Claim 53 corresponds to claim 44 and is rejected for the same reason as given above.

Claims 45 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Katoh (US Patent No. 5,949,757), Li (US Patent No. 5,473,599), Ko (US Patent No. 6,7879,202), and Galloway (US Patent No. 5,430,709).

Regarding claim 45, the combination further shows wherein said monitor/regulator tracks differences between outbound transmission control protocol (TCP) synchronize (SYN) and inbound response packets (ACKs) and determines whether the first network domain is sourcing undesirable network traffic based on said differences (see Poletto, pp. 16-17).

The combination does not show tracking differences between finish (FIN) packets and inbound response packets.

Galloway shows that finish (FIN) packets should elicit ACK packets in response (see Fig. 3). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto, Katoh, Li, and Ko to track FIN packets in order to provide an additional basis for determining that traffic is malicious.

Claim 54 corresponds to claim 45 and is rejected for the same reason as given above.

Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Ko (US Patent No. 6,789,202).

Regarding claim 48, Malan shows a network comprising:

- a first network domain (for example, an enterprise network: see first paragraph under "StormDetector" on p. 12);
- a second network domain (ISP-B: see Fig. 2 on p. 13 of Malan);

- a first routing device (comprising an attacker's router) at a boundary between the first network domain and public internetworking fabric (comprising an ISP network: see Fig. 4 and the paragraph spanning pp. 14-15) to route network traffic between the first network domain and the public internetworking fabric; (implicitly disclosed as the typical functionality of a first-hop router: see last paragraph on p. 12) and
- a second network domain (ISP-B) including a second routing device (comprising a router in ISP-B) for routing network traffic out of and into the second network domain (see Fig. 2 on p. 13 of Malan);
- a monitor/regulator (comprising the StormDetector analysis engine) that monitors the network traffic routed by said first routing device and said second routing device (comprising "flow statistics": see second and third paragraphs under "StormDetector" on p. 12 and note that StormDetector can be used in "source and transit networks" and "an attacker's originating network"), and determines if at least a selected one of the first and second network domains is sourcing undesirable network traffic out of the selected one of the first and second network domains (note that the system of Malan monitors traffic statistics sent from ISP routers: see second paragraph on p. 11 and Fig. 2 of Malan) based on network traffic characteristics observed of network traffic routed through said first and second routing devices (comprising determining that the first network is the location of the attacker: see "StormDetector" on p. 12 of Malan).

Malan does not explicitly show wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least one of said first and second network domains, lowers a threshold for concluding that undesirable network traffic are being sourced out of an other one of said first and second network domains.

Ko shows a upon determining a network attack is occurring at one network domain (e.g., detecting an attack by a "critical sensor" at a first local network: see col. 5, lines 9-13; and Fig. 1, depicting the sensors in each local network 108), lowers a threshold for concluding that a network attack is occurring at another network domain (parameters sent to the lower-level sensors "can be changed to more conservative values during an attack"; in the example given, the system concludes that fewer password tries are necessary to trigger a security response at a second local network; see col. 4, lines 30-39 and col. 5, lines 7-46). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan to lower thresholds in response to determining attacks as taught by Ko in order to allow respond more quickly to a large-scale coordinated attack (see Ko, col. 5, lines 43-46).

Claim 58 is rejected under 35 U.S.C. 103(a) as being unpatentable over Malan (US Pub. No. 2002/0032871) in view of Poletto (US Pub. No. 2002/0032880), and further in view of Katoh (US Patent No. 5,949,757) and Ko (US Patent No. 6,7879,202).

Regarding claim 58, Malan shows a network comprising:

- a network domain which is a local area network (for example, an enterprise network: see first paragraph under "StormDetector" on p. 12);

- a routing device (comprising an attacker's router) in the local area network at a boundary between the local area network and public internetworking fabric (comprising an ISP network: see Fig. 4 and the paragraph spanning pp. 14-15) to route network traffic between the network domain and the public internetworking fabric (implicitly disclosed as the typical functionality of a first-hop router: see last paragraph on p. 12); and
- a monitor/regulator (comprising the StormDetector analysis engine), either integrally disposed in said routing device or coupled to the routing device (see second paragraph under "StormDetector" on p. 12 and Figs. 2 and 4), to monitor the network traffic routed by said routing device by analyzing flow records (comprising "flow statistics": see second and third paragraphs under "StormDetector" on p. 12 and note that StormDetector can be used in "source and transit networks" and "an attacker's originating network") describing traffic conversation as indicated by a combination of source and destination addresses received from the routing device (comprising "flow statistics" as described above, further explained as being indicated by a combination of source and destination addresses in the paragraph spanning pp. 3-4), the monitor/regulator determining if the network domain is sourcing undesirable network traffic (comprising determining that the attack originates in the enterprise network: see paragraph spanning pp. 14-15) that is originating in the network domain and being routed out of the network domain by the routing device (note that the attacker must send the traffic out of the enterprise network in order for it to reach the web host), the monitor/regulator generating statistics concerning destination addresses to

determine whether the network domain is sourcing the undesirable network traffic (see discussion of "flow-based statistics," including "destination address," in paragraph spanning pp. 3-4 of Malan), wherein said monitor/regulator instructs the routing device to slow the undesirable network traffic (comprising slowing the attack traffic to zero with instructions to the router that block traffic: see paragraph spanning pp. 14-15 of Malan;

- wherein the undesirable network traffic comprises a denial of service attack in which the undesirable network traffic is launched against a target network device (for example, a target web hosting server: see "StormDetector" on p. 12 and "StormBreaker" on p. 14) in order to undermine the operation of that target network device by overwhelming the target network device with network traffic (typical of denial of service attacks, and further explained at the first paragraph on p. 3), out of the network domain (note that the attacker must send the traffic out of the enterprise network in order for it to reach the web host),
- wherein said monitor/regulator instructs the routing device to mitigate the undesirable network traffic (by "blocking" it) that is being sourced from the network domain in response to making said determination that the network domain is sourcing the undesirable network traffic (see discussion of "StormBreaker" at p. 14).

Malan does not *explicitly* show wherein said monitor/regulator makes said determination based at least in part on differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

Poletto shows identifying malicious traffic at a routing device (comprising a gateway) based on differential characteristics (comprising a ratio of request packets to acknowledgement packets) between request packets routed out of said network domain (comprising client request packets which are routed out of an attacker's domain), and response packets routed into the network domain (comprising server acknowledgement packets which are routed into the attacker's domain: see pages 15-16). Because both Malan and Poletto teach methods for identifying malicious traffic at a routing device, it would have been obvious to one of ordinary skill in the art to substitute one method for the other in order to achieve the predictable result of determining that the network domain is sourcing undesirable traffic.

Malan in view of Poletto does not explicitly show wherein the instruction to mitigate the undesirable network traffic is to lower the priority of the undesirably network traffic.

Katoh teaches lowering the priority of undesirable traffic as an alternative to blocking it outright (see col. 4, lines 10-13). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Malan in view of Poletto to lower the priority of undesirable traffic as taught by Katoh in order to ease congestion caused by the attack without running the risk of blocking innocent traffic entirely.

Malan in view of Poletto and Katoh does not explicitly show wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least one of said first and second network domains, lowers a threshold for concluding that undesirable network traffic are being sourced out of an other one of said first and second network domains.

Ko shows upon determining a network attack is occurring at one network domain (e.g., detecting an attack by a "critical sensor" at a first local network: see col. 5, lines 9-13; and Fig. 1, depicting the sensors in each local network 108), lowering a threshold for concluding that a network attack is occurring at another network domain (parameters sent to the lower-level sensors "can be changed to more conservative values during an attack"; in the example given, the system concludes that fewer password tries are necessary to trigger a security response at a second local network; see col. 4, lines 30-39 and col. 5, lines 7-46). It would have been obvious to one of ordinary skill in the art at the time of the invention to further the system of Malan in view of Poletto and Katoh to lower thresholds in response to determining attacks as taught by Ko in order to allow respond more quickly to a large-scale coordinated attack (see Ko, col. 5, lines 43-46).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher D. Biagini whose telephone number is (571)272-9743. The examiner can normally be reached on weekdays from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher Biagini
(571) 272-9743

/HASSAN PHILLIPS/
Primary Examiner, Art Unit 2445